

No.	Time	Source	Destination
1	0.000000	145.254.160.237	65.208.228.223
62	tip2 > http [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1		TCP

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)

Encapsulation type: Ethernet (1)

Arrival Time: May 13, 2004 06:17:07.311224000 EDT

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1084443427.311224000 seconds

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 0.000000000 seconds]

Frame Number: 1

Frame Length: 62 bytes (496 bits)

Capture Length: 62 bytes (496 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ip:tcp]

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || tcp.port == 80]

Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)

Destination: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)

Address: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)

.... ..1. = LG bit: Locally administered address (this is NOT the factory default)

.... ..0 = IG bit: Individual address (unicast)

Source: Xerox_00:00:00 (00:00:01:00:00:00)

Address: Xerox_00:00:00 (00:00:01:00:00:00)

.... ..0. = LG bit: Globally unique address (factory default)

.... ..0 = IG bit: Individual address (unicast)

Type: IP (0x0800)

Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)

Total Length: 48

Identification: 0x0f41 (3905)

Flags: 0x02 (Don't Fragment)

0... = Reserved bit: Not set

.1.. = Don't fragment: Set

```

    ..0. .... = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x91eb [correct]
    [Good: True]
    [Bad: False]
Source: 145.254.160.237 (145.254.160.237)
Destination: 65.208.228.223 (65.208.228.223)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http
(80), Seq: 0, Len: 0
Source port: tip2 (3372)
Destination port: http (80)
[Stream index: 0]
Sequence number: 0      (relative sequence number)
Header length: 28 bytes
Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..1. = Syn: Set
    [Expert Info (Chat/Sequence): Connection establish request
(SYN): server port http]
        [Message: Connection establish request (SYN): server
port http]
            [Severity level: Chat]
            [Group: Sequence]
    .... .... ...0 = Fin: Not set
Window size value: 8760
[Calculated window size: 8760]
Checksum: 0xc30c [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-
Operation (NOP), SACK permitted
    Maximum segment size: 1460 bytes
        Kind: MSS size (2)
        Length: 4
        MSS Value: 1460
    No-Operation (NOP)
        Type: 1
            0... .... = Copy on fragmentation: No
            .00. .... = Class: Control (0)

```

```

...0 0001 = Number: No-Operation (NOP) (1)
No-Operation (NOP)
  Type: 1
    0... .... = Copy on fragmentation: No
    .00. .... = Class: Control (0)
    ...0 0001 = Number: No-Operation (NOP) (1)
TCP SACK Permitted Option: True
  Kind: SACK Permission (4)
  Length: 2

```

```

0000  fe ff 20 00 01 00 00 00 01 00 00 00 08 00 45
00    .. .....E.
0010  00 30 0f 41 40 00 80 06 91 eb 91 fe a0 ed 41 d0  .
0.A@.....A.
0020  e4 df 0d 2c 00 50 38 af fe 13 00 00 00 00 70
02    ....,P8.....p.
0030  22 38 c3 0c 00 00 02 04 05 b4 01 01 04 02          "8.....

```

No.	Time	Source	Destination
62	0.911310	65.208.228.223	145.254.160.237
Protocol Length Info			
62	http > tip2 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380		
SACK_PERM=1			

```

Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: May 13, 2004 06:17:08.222534000 EDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1084443428.222534000 seconds
  [Time delta from previous captured frame: 0.911310000 seconds]
  [Time delta from previous displayed frame: 0.911310000 seconds]
  [Time since reference or first frame: 0.911310000 seconds]
  Frame Number: 2
  Frame Length: 62 bytes (496 bits)
  Capture Length: 62 bytes (496 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ip:tcp]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80]
Ethernet II, Src: fe:ff:20:00:01:00 (fe:ff:20:00:01:00), Dst:
Xerox_00:00:00 (00:00:01:00:00:00)
  Destination: Xerox_00:00:00 (00:00:01:00:00:00)
  Address: Xerox_00:00:00 (00:00:01:00:00:00)
    .... ..0. .... .... .... = LG bit: Globally unique
address (factory default)
    .... ..0 .... .... .... = IG bit: Individual address
(unicast)
  Source: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
  Address: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)

```

```

.....1. .... = LG bit: Locally administered
address (this is NOT the factory default)
.....0 .... = IG bit: Individual address
(unicast)
Type: IP (0x0800)
Internet Protocol Version 4, Src: 65.208.228.223 (65.208.228.223),
Dst: 145.254.160.237 (145.254.160.237)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00: Not-ECT (Not ECN-Capable Transport))
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.....00 = Explicit Congestion Notification: Not-ECT (Not
ECN-Capable Transport) (0x00)
Total Length: 48
Identification: 0x0000 (0)
Flags: 0x02 (Don't Fragment)
0... .... = Reserved bit: Not set
.1.. .... = Don't fragment: Set
..0. .... = More fragments: Not set
Fragment offset: 0
Time to live: 47
Protocol: TCP (6)
Header checksum: 0xf22c [correct]
[Good: True]
[Bad: False]
Source: 65.208.228.223 (65.208.228.223)
Destination: 145.254.160.237 (145.254.160.237)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: http (80), Dst Port: tip2
(3372), Seq: 0, Ack: 1, Len: 0
Source port: http (80)
Destination port: tip2 (3372)
[Stream index: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
Header length: 28 bytes
Flags: 0x012 (SYN, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 .... = Acknowledgment: Set
.... .... 0... = Push: Not set
.... .... .0.. = Reset: Not set
.... .... ..1. = Syn: Set
[Expert Info (Chat/Sequence): Connection establish
acknowledge (SYN+ACK): server port http]

```

[Message: Connection establish acknowledge (SYN+ACK):
server port http]

[Severity level: Chat]

[Group: Sequence]

....0 = Fin: Not set

Window size value: 5840

[Calculated window size: 5840]

Checksum: 0x5bdc [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted

Maximum segment size: 1380 bytes

Kind: MSS size (2)

Length: 4

MSS Value: 1380

No-Operation (NOP)

Type: 1

0... = Copy on fragmentation: No

.00. = Class: Control (0)

...0 0001 = Number: No-Operation (NOP) (1)

No-Operation (NOP)

Type: 1

0... = Copy on fragmentation: No

.00. = Class: Control (0)

...0 0001 = Number: No-Operation (NOP) (1)

TCP SACK Permitted Option: True

Kind: SACK Permission (4)

Length: 2

[SEQ/ACK analysis]

[This is an ACK to the segment in frame: 1]

[The RTT to ACK the segment was: 0.911310000 seconds]

0000 00 00 01 00 00 00 fe ff 20 00 01 00 08 00 45

00E.

0010 00 30 00 00 40 00 2f 06 f2 2c 41 d0 e4 df 91 fe .

0..@./...,A.....

0020 a0 ed 00 50 0d 2c 11 4c 61 8b 38 af fe 14 70 12 ...P.,.La.

8...p.

0030 16 d0 5b dc 00 00 02 04 05 64 01 01 04 02 ..[.....d....

No.	Time	Source	Destination
Protocol Length Info			
3	0.911310	145.254.160.237	65.208.228.223 TCP
54	tip2 > http [ACK] Seq=1 Ack=1 Win=9660 Len=0		

Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

Encapsulation type: Ethernet (1)

Arrival Time: May 13, 2004 06:17:08.222534000 EDT

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1084443428.222534000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.911310000 seconds]
Frame Number: 3
Frame Length: 54 bytes (432 bits)
Capture Length: 54 bytes (432 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ip:tcp]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80]
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
Destination: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
Address: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
.... ..1. = LG bit: Locally administered address (this is NOT the factory default)
.... ..0 = IG bit: Individual address (unicast)
Source: Xerox_00:00:00 (00:00:01:00:00:00)
Address: Xerox_00:00:00 (00:00:01:00:00:00)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0 = IG bit: Individual address (unicast)
Type: IP (0x0800)
Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
Total Length: 40
Identification: 0x0f44 (3908)
Flags: 0x02 (Don't Fragment)
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x91f0 [correct]
[Good: True]
[Bad: False]
Source: 145.254.160.237 (145.254.160.237)
Destination: 65.208.228.223 (65.208.228.223)

```

[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http
(80), Seq: 1, Ack: 1, Len: 0
Source port: tip2 (3372)
Destination port: http (80)
[Stream index: 0]
Sequence number: 1      (relative sequence number)
Acknowledgment number: 1  (relative ack number)
Header length: 20 bytes
Flags: 0x010 (ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
Window size value: 9660
[Calculated window size: 9660]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x7964 [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
[SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 2]

```

```

0000  fe ff 20 00 01 00 00 00 01 00 00 00 08 00 45
00    .. .....E.
0010  00 28 0f 44 40 00 80 06 91 f0 91 fe a0 ed 41 d0  .
(.D@.....A.
0020  e4 df 0d 2c 00 50 38 af fe 14 11 4c 61 8c 50
10    ...,P8....La.P.
0030  25 bc 79 64 00 00                                %.yd..

```

No.	Time	Source	Destination
4	0.911310	145.254.160.237	65.208.228.223
533	GET /download.html	HTTP/1.1	HTTP

```

Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
Encapsulation type: Ethernet (1)
Arrival Time: May 13, 2004 06:17:08.222534000 EDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1084443428.222534000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]

```

[Time since reference or first frame: 0.911310000 seconds]
Frame Number: 4
Frame Length: 533 bytes (4264 bits)
Capture Length: 533 bytes (4264 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ip:tcp:http]
[Number of per-protocol-data: 1]
[Hypertext Transfer Protocol, key 0]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80]
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
Destination: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
Address: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
.... ..1. = LG bit: Locally administered address (this is NOT the factory default)
.... ..0 = IG bit: Individual address (unicast)
Source: Xerox_00:00:00 (00:00:01:00:00:00)
Address: Xerox_00:00:00 (00:00:01:00:00:00)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0 = IG bit: Individual address (unicast)
Type: IP (0x0800)
Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
Total Length: 519
Identification: 0x0f45 (3909)
Flags: 0x02 (Don't Fragment)
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x9010 [correct]
[Good: True]
[Bad: False]
Source: 145.254.160.237 (145.254.160.237)
Destination: 65.208.228.223 (65.208.228.223)
[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 1, Ack: 1, Len: 479
Source port: tip2 (3372)
Destination port: http (80)
[Stream index: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 480 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Header length: 20 bytes
Flags: 0x018 (PSH, ACK)
 000. = Reserved: Not set
 ...0 = Nonce: Not set
 0... = Congestion Window Reduced (CWR): Not set
 0.. = ECN-Echo: Not set
 0. = Urgent: Not set
 1 = Acknowledgment: Set
 1... = Push: Set
 0.. = Reset: Not set
 0. = Syn: Not set
 0 = Fin: Not set
Window size value: 9660
[Calculated window size: 9660]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0xa958 [validation disabled]
 [Good Checksum: False]
 [Bad Checksum: False]
[SEQ/ACK analysis]
 [Bytes in flight: 479]
Hypertext Transfer Protocol
GET /download.html HTTP/1.1\r\n
 [Expert Info (Chat/Sequence): GET /download.html HTTP/1.1\r\n]
 [Message: GET /download.html HTTP/1.1\r\n]
 [Severity level: Chat]
 [Group: Sequence]
Request Method: GET
Request URI: /download.html
Request Version: HTTP/1.1
Host: www.ethereal.com\r\n
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1\r\n
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip,deflate\r\n
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
Keep-Alive: 300\r\n
Connection: keep-alive\r\n
Referer: http://www.ethereal.com/development.html\r\n

\r\n
[Full request URI: http://www.ethereal.com/download.html]
[HTTP request 1/1]
[Response in frame: 38]

0000	fe ff 20 00 01 00 00 00 01 00 00 00 08 00 45	
00E.	
0010	02 07 0f 45 40 00 80 06 90 10 91 fe a0 ed 41	
d0	...E@.....A.	
0020	e4 df 0d 2c 00 50 38 af fe 14 11 4c 61 8c 50	
18	...,P8....La.P.	
0030	25 bc a9 58 00 00 47 45 54 20 2f 64 6f 77 6e 6c	%..X..GET /
downl		
0040	6f 61 64 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e	oad.html HTTP/
1.		
0050	31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 65 74 68	1..Host:
www.eth		
0060	65 72 65 61 6c 2e 63 6f 6d 0d 0a 55 73 65 72 2d	
ereal.com..User-		
0070	41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35	Agent:
Mozilla/5		
0080	2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20	.0 (Windows;
U;		
0090	57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20	Windows NT
5.1;		
00a0	65 6e 2d 55 53 3b 20 72 76 3a 31 2e 36 29 20 47	en-US; rv:1.6)
G		
00b0	65 63 6b 6f 2f 32 30 30 34 30 31 31 33 0d 0a 41	ecko/
20040113..A		
00c0	63 63 65 70 74 3a 20 74 65 78 74 2f 78 6d 6c 2c	ccept: text/
xml,		
00d0	61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2c	application/
xml,		
00e0	61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d	application/
xhtm		
00f0	6c 2b 78 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b	l+xml,text/
html;		
0100	71 3d 30 2e 39 2c 74 65 78 74 2f 70 6c 61 69 6e	q=0.9,text/
plain		
0110	3b 71 3d 30 2e 38 2c 69 6d 61 67 65 2f 70 6e 67	;q=0.8,image/
png		
0120	2c 69 6d 61 67 65 2f 6a 70 65 67 2c 69 6d 61 67	,image/
jpeg,imag		
0130	65 2f 67 69 66 3b 71 3d 30 2e 32 2c 2a 2f 2a 3b	e/gif;q=0.2,*/
*/		
0140	71 3d 30 2e 31 0d 0a 41 63 63 65 70 74 2d 4c 61	q=0.1..Accept-
La		
0150	6e 67 75 61 67 65 3a 20 65 6e 2d 75 73 2c 65 6e	nguage: en-
us,en		
0160	3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d	

```

45      ;q=0.5..Accept-E
0170  6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 64 65      ncoding:
gzip,de
0180  66 6c 61 74 65 0d 0a 41 63 63 65 70 74 2d 43 68      flate..Accept-
Ch
0190  61 72 73 65 74 3a 20 49 53 4f 2d 38 38 35 39 2d      arset:
ISO-8859-
01a0  31 2c 75 74 66 2d 38 3b 71 3d 30 2e 37 2c 2a 3b
1,utf-8;q=0.7,*;
01b0  71 3d 30 2e 37 0d 0a 4b 65 65 70 2d 41 6c 69 76      q=0.7..Keep-
Aliv
01c0  65 3a 20 33 30 30 0d 0a 43 6f 6e 6e 65 63 74 69      e:
300..Connecti
01d0  6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a      on: keep-
alive..
01e0  52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f      Referer:
http://
01f0  77 77 77 2e 65 74 68 65 72 65 61 6c 2e 63 6f 6d
www.ethereal.com
0200  2f 64 65 76 65 6c 6f 70 6d 65 6e 74 2e 68 74 6d      /
development.htm
0210  6c 0d 0a 0d 0a                                          l....

```